

19 Sonrası...

Geleceği
yeniden
keşfetmek

Yeni dönem, yeni siber
güvenlik stratejisi

Ulvi Cemal Bucak

22.12.2020

Küresel Dijital Dünyada Güven Araştırması

2021



Araştırma, Temmuz - Ağustos 2020 tarihleri arasında 3.249 teknoloji ve şirket yöneticisi ile gerçekleştirildi.

Anket Katılımcıları:



%73 C-level yönetici



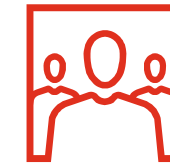
%50/50 Şirket ve Teknoloji yöneticileri



%10 Bilgi Güvenliği Yöneticileri



%50 büyük şirketlerde çalışan yöneticiler (1 milyar\$ ve üzeri geliri olan şirketler)



%28 Kadın katılımcı



Araştırma bulguları, siber güvenlikte nelerin değiştiğini ve gelecekte nelerin beklediğini ortaya koyuyor.

Bölgeler



Batı Avrupa (%34), Kuzey Amerika (%29), Asya Pasifik (%18), Latin Amerika (%8), Doğu Avrupa (%4), Orta Doğu (%3) ve Afrika (%3)

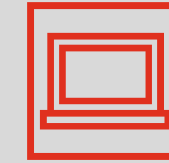
Sektörler



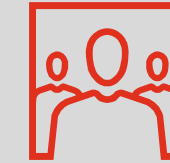
%22 Teknoloji, medya, telekomünikasyon



%19 Endüstriyel üretim



%20 Perakende ve tüketici ürünleri



%8 Sağlık

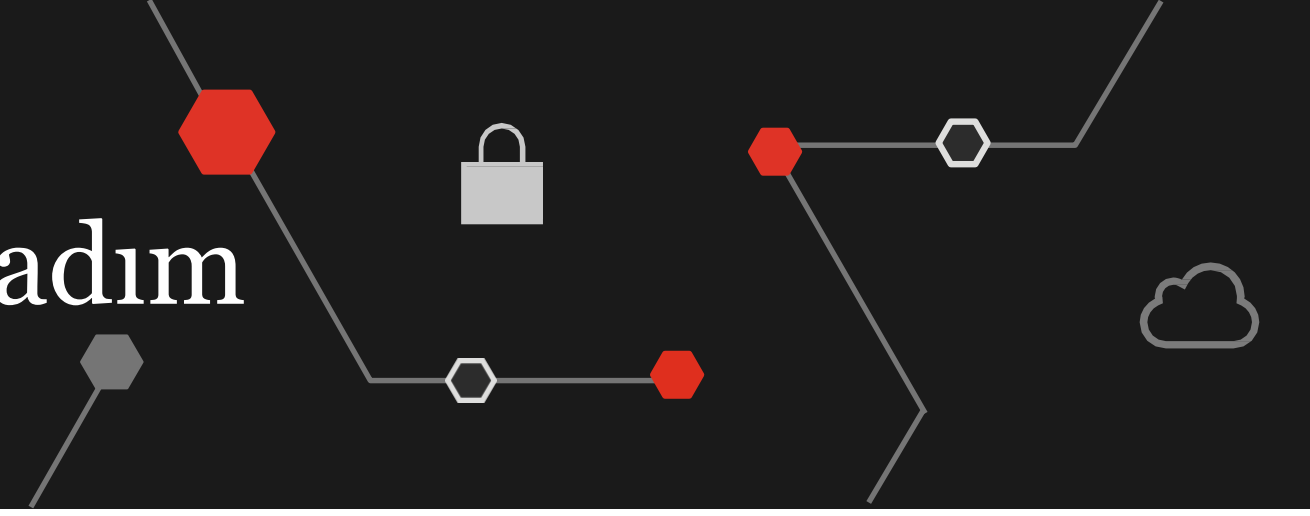




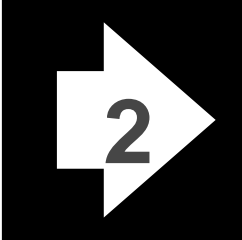

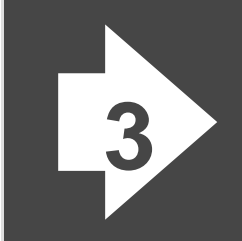




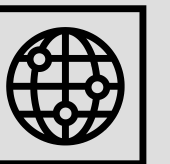
%19 Finansal hizmetler



%8 Enerji, altyapı ve doğal kaynaklar

Siber g venlikte bir sonraki seviyeye ge mek i in be  adım



-  Siber g venlik stratejinizi ba tan planlayın, liderliđi bu yeni d neme hazırlayın. 
-  Siber risklerle daha iyi m cadele etmek i in b t enizi g zden ge irin. 
-  Siber saldırganlarla e it  artlarda m cadele edebilmek i in her olanađı deđerlendirin. 
-  Her t rl  senaryo i in dayanıklı bir yapı kurun. 
-  Siber g venlik ekibinizi geleceđe hazırlayın. 

The background is a dark gray field with a light gray hexagonal grid. A network of lines connects various points, some of which are marked with red hexagons and others with gray hexagons. Scattered throughout the grid are several icons: a cloud, a padlock, and a shield. The text is centered within a red rectangular box.

Siber güvenlik stratejinizi
baştan planlayın

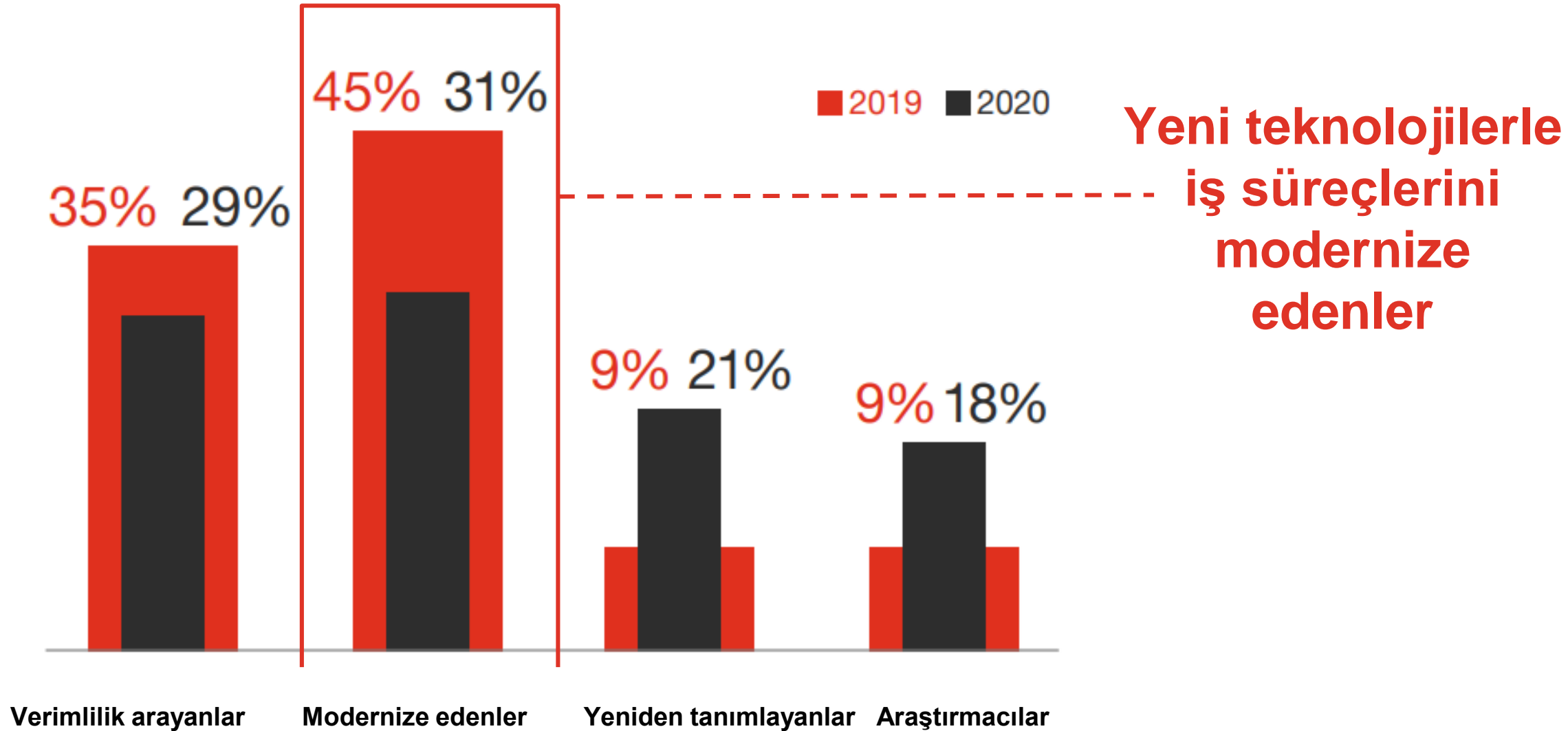
Şirketlerin dijital dönüşümü çok daha kapsamlı ve hızlı

%40

Dijital dönüşüm sürecini hızlandıranlar
- daha önce gündeme almadıkları iş stratejilerini hayata geçiriyorlar

%21

İş yapış biçimlerini değiştirip,
organizasyon yapılarını yeniden tanımlayanlar



İpucu

1. Yeni teknolojiler + yeni iş modelleri = yeni riskler.
2. Siber güvenlik, hızlı seyreden dijital dönüşümün çok daha güvenli bir şekilde tamamlanmasına yardımcı olur.
3. Maliyetleri düşürmek için otomasyonu artırmak tercih ediliyor.

Siber stratejileri sıfırdan tasarlama zamanı

COVID-19 sebebiyle aşağıdaki değişimlerden hangilerinin sektörünüzdeki siber güvenlik yapısı üzerinde etkili olmasını bekliyorsunuz?

Siber güvenlik işle ilgili kararların veya planların bir parçası haline geldi

50%

Siber harcamalar ve yatırımlar için yeni bütçe planları

44%

Daha etkin ve detaylı siber risk ölçümlmeleri

44%

Yönetim kurulları ve CEO ile CISO arasında daha etkin iletişim

43%

Düşük ihtimalli ama büyük etkili saldırılar için dayanıklılık testleri

43%

Geçen seneki araştırmamızdan bugüne %25 artış

%96

COVID-19 sebebiyle siber güvenlik stratejilerini güncelleyeceğini belirten katılımcı oranı



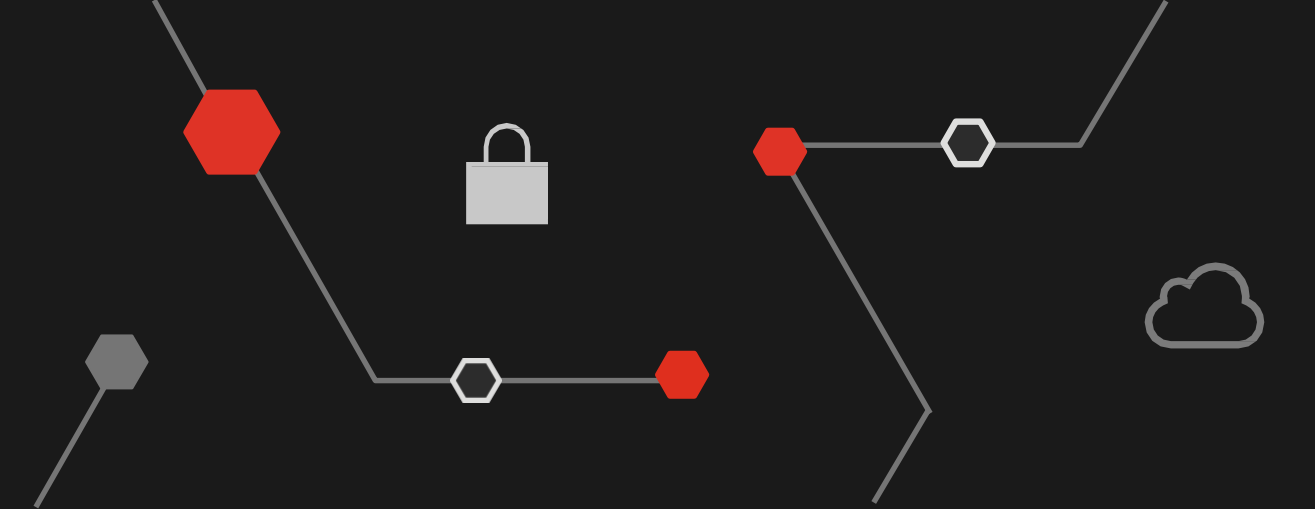
Temel bulgular

1. İş odaklı bir siber güvenlik stratejisi geliştirin.
2. Yalnızca BT departmanınızın değil, şirketinizin de vizyon ve hedefleriyle örtüşen bir strateji edinin.
3. Şirketinizin değerlerini koruyup, yeni değerler oluşturmaya yardımcı olacak stratejilerle dijital dünyada güvenin temsilcisi olun.



Siber bütçenizi gözden geçirin

Bütçenizi daha iyi değerlendirin



%64

Gelirlerinde düşüş bekliyor

%55

Siber güvenlik bütçesini artırmayı planlıyor

%51

2021'de tam zamanlı siber güvenlik istihdamı planlıyor

%55

Siber güvenlik harcamaların en önemli risklere karşı yeterli olmadığını düşünüyor

“Siber güvenlik için harcanan her bir kuruş şirketler dijitalleştikçe daha da değerlendiriliyor. Çünkü her yeni dijital süreç ve ürün, yeni bir siber risk anlamına geliyor.”

Siber riskler ölçüldü, bütçeler optimize edildi

%17

Siber güvenlik risklerini ölçen ve bunun faydasını görenler

%60

Siber güvenlik risk ölçümüne başlayan veya bunu geniş ölçekte uygulayanlar

- %17 önümüzdeki iki yıl içinde risk ölçümüne başlamayı planlıyor



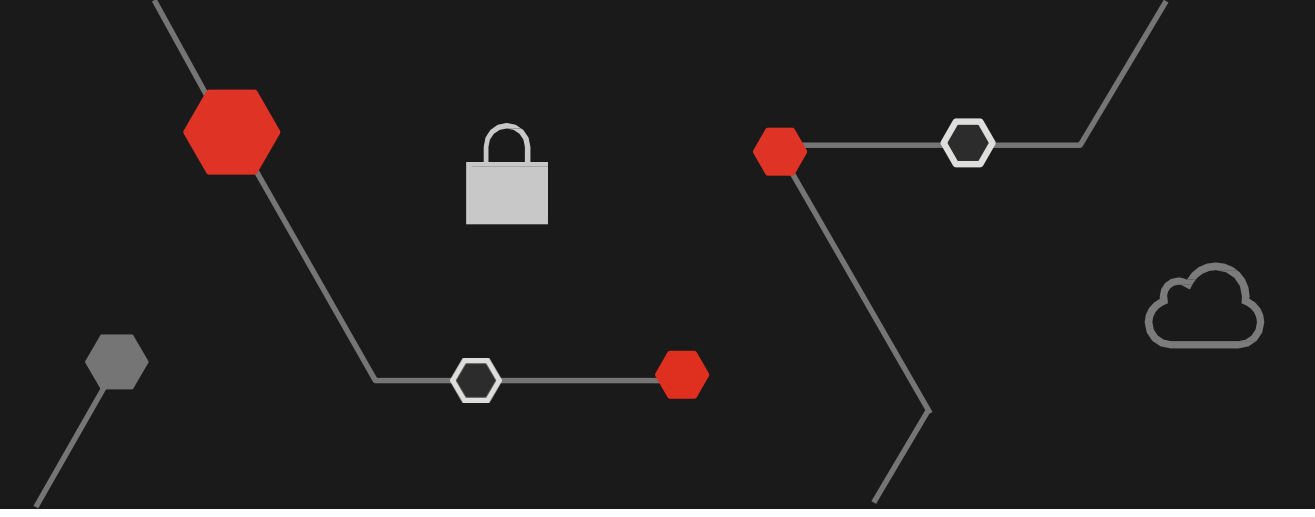
Temel bulgular

1. Siber güvenlik risk ölçümü önemlidir.
2. Siber bütçenizi şirket veya iş birimi bütçeleri ile ilişkilendirin.
3. Her siber proje yatırımının yaratacağı maddi karşılığı hesaplayın.



Siber saldırganlarla eşit
şartlarda mücadele edin

Yeni teknolojiler siber suçlara ortam sağlıyor



Siber güvenliğin iyileştirilmesine yardımcı olacak üç yeni yaklaşım



Siber güvenlik çalışanlarının beceri setlerini iyileştirmek



Siber güvenlik önlemlerinin etkinliğinin gerçek zamanlı takibi



Modern kimlik ve erişim yönetimi

10 milyar dolar üzeri gelir elde eden şirket yöneticileri, bu güvenlik modellerini ve teknolojilerinden faydalanıyor



Sıfır Güven (Zero Trust)



Sanallaştırma



Güvenlik hizmetleri yönetimi



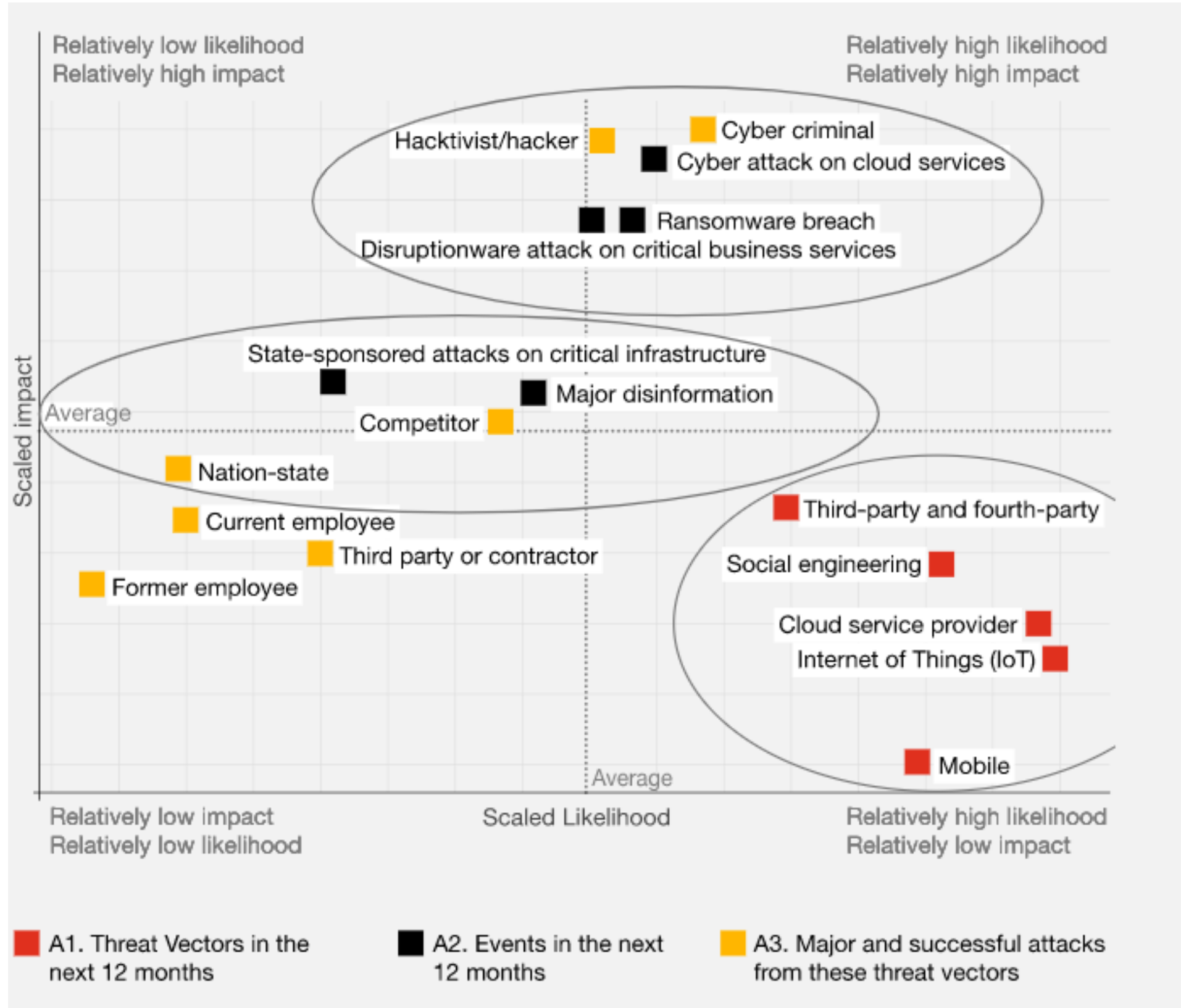
Bulut teknolojilerinin hızlandırılmış şekilde adaptasyonu



Her türlü senaryo için dayanıklı
bir yapı kurun

2021 yılının siber tehdit dünyası

Tehditler, aktörler ve olaylar: Göreceli olasılıkları ve etkileri



Tehditler

- Hacktivistler / Hackerlar
- Siber suçlular

Olaylar:

- Bulut tabanlı hizmetlere siber saldırılar
- Fidye yazılımı ihlalleri
- Kritik hizmetlere yönelik yıkıcı yazılım saldırıları

■ Büyük ve başarılı olması muthemel tehditler

■ Gelecek 12 ayda beklenen olaylar

Tehditler karşısında ne kadar güvendesiniz?

%40

yıkıcı bir siber saldırı meydana geldiğinde, kritik iş süreçlerinin çalışır durumda kalmasını sağlamak hazırlık yapmayı planları

%76

"Doğru yapılması durumunda, değerlendirme ve testlerin siber güvenlik yatırım hedeflemelerine yardımcı olabileceğini" düşünenler



Temel bulgular

1. Değerlendirme ve testleri uygulamayı gözden geçirin.
2. İyi bir siber güvenlik stratejisi, tehditlerin önüne geçmek için önemlidir.
3. İleriye dönük olarak, çoğu şirketin önceliği siber saldırı durumunda iş devamlılığını, acil durum yönetimini ve kriz yönetimini koordine etmek olacak.

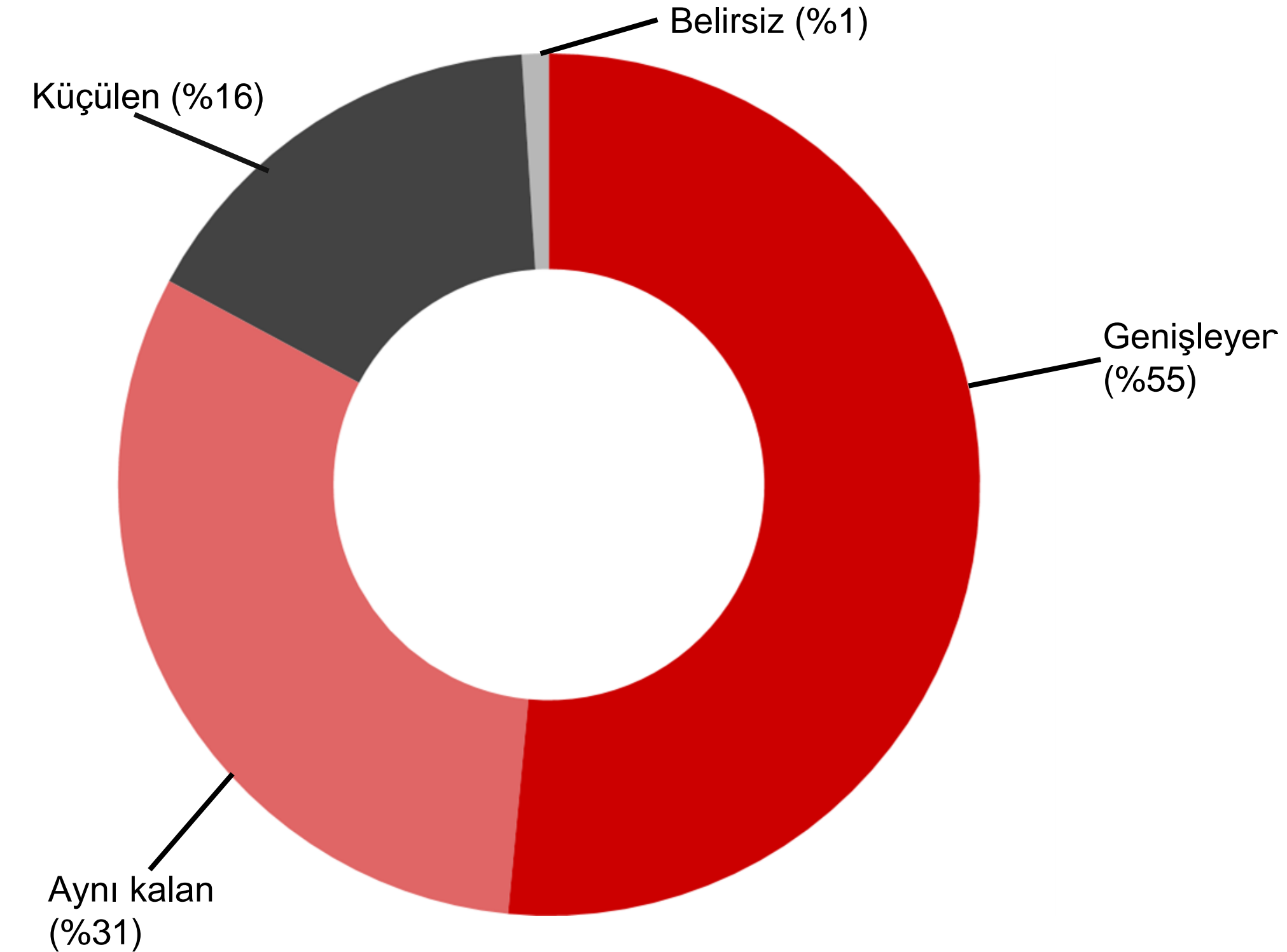
The background is a dark gray field with a light gray hexagonal grid. A network of lines connects various points, some of which are marked with red hexagons and others with gray hexagons. Scattered throughout the grid are several icons: a padlock, a cloud, and a small red triangle.

Siber güvenlik ekibinizi
geleceğe hazırlayın

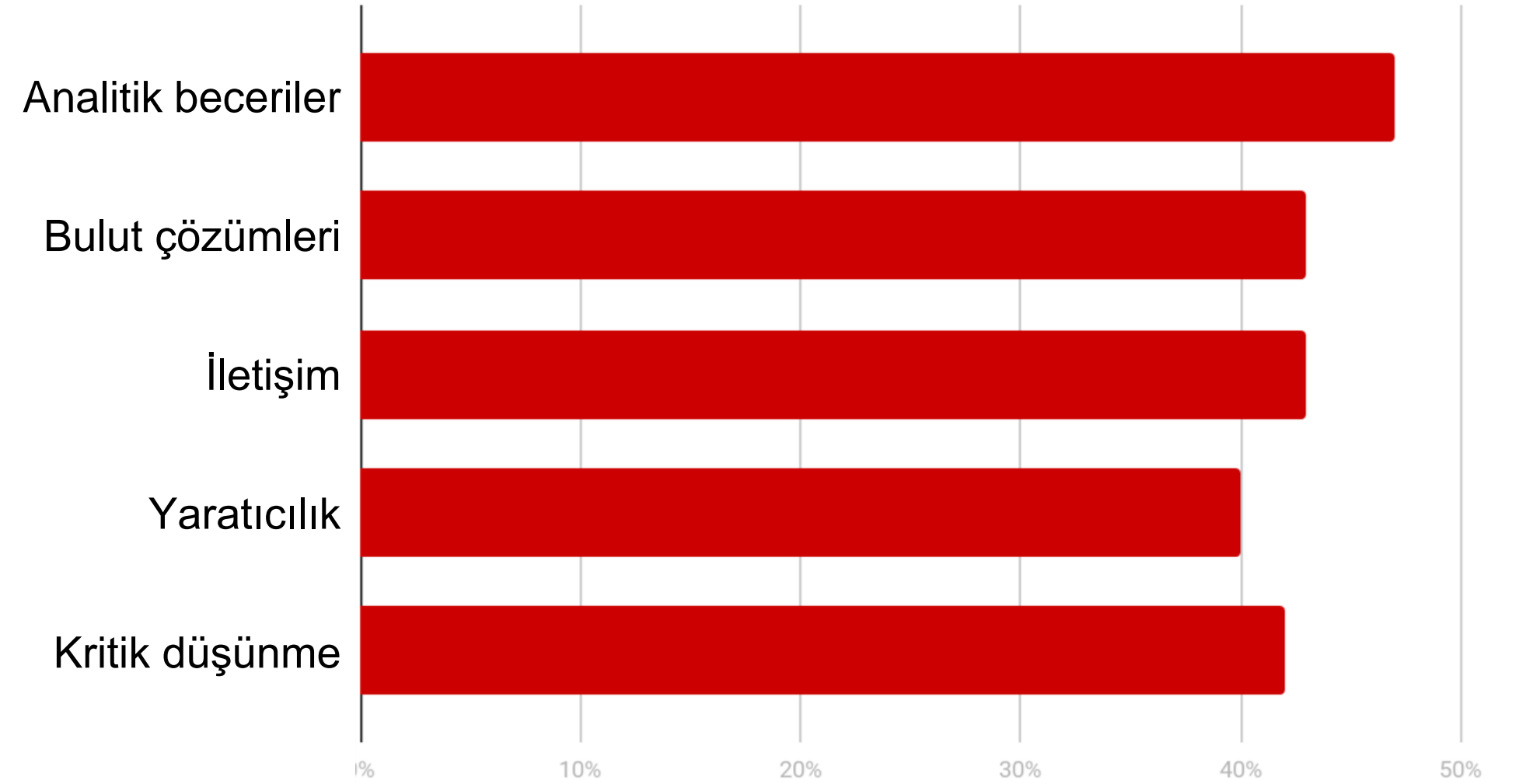
Ekibinizi genişletin ve geliştirin



Katılımcıların %55'i ekiplerini genişletmeyi planlıyor



Yaratıcılık, iletişim ve kritik düşünme becerileri büyük önem taşıyor



Yetenek ihtiyacını göz önünde bulundurun

%72

Mesleki öğrenmeye haftada 3 saatten daha fazla zaman ayıranlar

%85

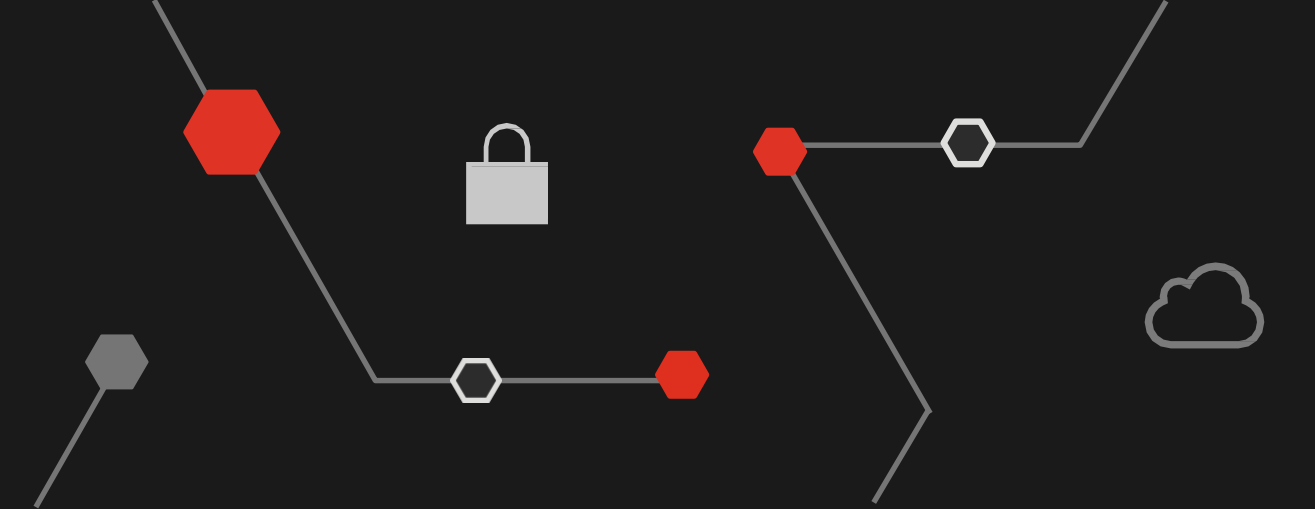
Yönetim hizmetlerini kullanan veya kullanmayı planlayanlar



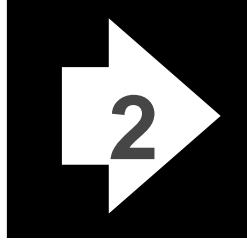

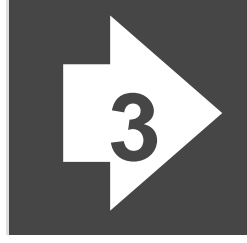

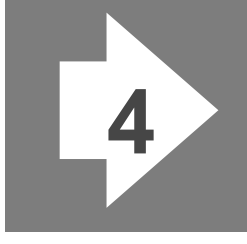


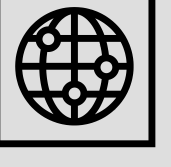


Temel Bulgular

1. İşe alım yaptığınız alandaki mevcut çalışanlarınızın becerilerini geliştirmeye odaklanın.
2. Çalışanı merkeze koyan, iş ve sonuç odaklı programlarla bunları destekleyin.
3. Yeni siber yetenekler için piyasada rekabet edecek kaynaklara sahip değilseniz, iyi bilinen bir güvenlik hizmetleri modeli edinmeyi düşünün.

Sonuç



-  Yalnızca BT departmanınızın değil, şirketinizin de vizyon ve hedefleriyle örtüşen bir strateji edinin. 
-  Riskin ölçülmesi, siber güvenlik yatırımlarınızın değerini iş hedeflerinize göre ölçmenize olanak tanır. 
-  Bulut güvenliği bir sonraki dönüm noktası. 
-  Siber güvenlik yatırımlarınızı doğru planlamak için risk değerlendirme ve güvenlik testlerine öncelik verin 
-  Siber yetenekleri kurumunza kazandırmakta zorlanıyorsanız güvenilir bir MSSP/CDC yaklaşımını değerlendirin 

19 Sonrası...

Geleceği
yeniden
keşfetmek

Teşekkürler

Ulvi Cemal Bucak

21.12.2020